

AFFIDAVIT IN SUPPORT OF APPLICATIONS FOR SEARCH WARRANTS

I, Joseph T. Gugliotta, being duly sworn, do hereby depose and say the following:

INTRODUCTION AND PURPOSE OF AFFIDAVIT

1. I am a U.S. Postal Inspector with the United States Postal Inspection Service (USPIS) and have been since 2006. I am assigned to the USPIS Boston Division where I am a member of the Mail Theft and Identity Theft Team, which investigates, among other things, financial crimes involving mail theft and the theft of personal identifiers and financial account numbers. During my employment as a U.S. Postal Inspector, I have conducted and participated in investigations of numerous financial crimes involving mail, bank, and wire fraud, as well as identity theft, money laundering, and counterfeit financial instruments.

2. As further discussed below, I am investigating Imanol RIOS-FRANCO and others for violations of 18 U.S.C. § 1704 (Theft or Forging of Postal Service Keys), 18 U.S.C. § 1708 (Theft or Receipt of Stolen Mail), 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1344 (Bank Fraud), and 18 U.S.C. § 371 (Conspiracy) (hereinafter, the “Target Offenses”).

3. I submit this affidavit in support of applications for warrants to search the following:

- a. A 2018 BMW X6 bearing Massachusetts registration 1WYZ17 and Vehicle Identification Number 5UXKU2C53J0Z61448 (“the Subject Vehicle”), which is in law enforcement custody and described in Attachment A-1. This vehicle is registered to Andrei Echeverria of A&E Lux Auto, LLC, a small rental car company with 11 vehicles registered to Echeverria. According to Commonwealth of Massachusetts records, Echeverria is listed as the Manager of A&E Lux Auto, LLC; and

- b. The Infotainment and Telematic System in the Subject Vehicle, (hereinafter, “the equipment”) described in Attachment A-2.

There is probable cause to believe that the Subject Vehicle and the equipment contain evidence, fruits, and instrumentalities of the Target Offenses, as described in Attachments B-1 and B-2.

4. The facts in this affidavit come from my personal review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter. The background of this investigation can be found in the February 26, 2024 Affidavit of Special Agent E. Austin Wozniak. I am incorporating Special Agent Wozniak’s Affidavit by reference and it is attached as Exhibit A. All times herein are approximate.

PROBABLE CAUSE

Search Warrant for RIOS-FRANCO’s Residence

5. Exhibit A was submitted, in part, to support applications for search warrants for RIOS-FRANCO’s residence at 3611 Washington Street, Unit B222, Jamaica Plain, Massachusetts 02130 (24-mj-4039-DHH) and RIOS-FRANCO’s person (24-mj-4038-DHH).

6. In preparation for the warrant, investigators reviewed security camera footage and conducted surveillance around RIOS-FRANCO’s residence. On February 2, 2024, at 1:20 p.m., investigators observed the Subject Vehicle stop outside 3611 Washington Street in front of the common entrance closest to Unit B222. At 1:40 p.m., investigators observed a masked subject wearing a black Moncler-brand jacket come from the garage entrance of 3611 Washington Street and enter the passenger side of the Subject Vehicle. On February 12 and 17, 2024, investigators observed RIOS-FRANCO wearing the same black Moncler-brand jacket coming and going from

RIOS-FRANCO's apartment. I believe that RIOS-FRANCO was a passenger in the Subject Vehicle on February 2, 2024.

7. On February 27, 2024, agents executed the search warrant for RIOS-FRANCO's residence and found him and his mother inside Unit B222 in the early morning. Investigators also found evidence of mail theft and card cracking in RIOS-FRANCO's residence including 17 debit cards in other people's names associated with accounts at different banks as well as a large number of checks in names of people not associated with B222 or RIOS-FRANCO. During my review of the large number of checks, I found a check written by a resident of Watertown, Massachusetts, dated January 11, 2024.¹ I also found a Bank of America ("BOA") ATM receipt showing the deposit of more than \$9,000 at a BOA ATM on February 22, 2024.

8. In my training and experience, the debit cards recovered from RIOS-FRANCO's residence are indicative of recruited accountholders who voluntarily provided access to their bank accounts to RIOS-FRANCO in exchange for a portion of funds fraudulently obtained by a check washing scheme. The large number of checks seized from RIOS-FRANCO's residence is indicative of a mail theft scheme, wherein individuals use an Arrow Key to open USPS mail collection boxes and steal checks dropped into a collection box. The BOA ATM receipt is evidence of the deposit of one or more stolen checks into a recruited accountholder's BOA account.

9. Finally, in my training and experience, people often date their checks on or about the day they mail them. The discovery of checks dated in January 2024 indicate to me that RIOS-FRANCO was in possession of stolen checks for at least one month.

¹ On January 9, 2024, I received a request from Watertown Police asking for assistance investigating a large number of Arrow Key-related mail theft incidents. As discussed in Exhibit A, Arrow Keys are used to open USPS mail collection boxes.

10. I have attached images below of the container seized from RIOS-FRANCO's residence that contained the numerous debit cards, stolen checks, and BOA ATM receipt.



11. Agents also found a BMW key fob in RIOS-FRANCO's residence. When I asked RIOS-FRANCO about this key fob, he said it belonged to his friend "YAZ" and that the vehicle was parked in a parking lot on a side street near the apartment building. RIOS-FRANCO said he has been friends with YAZ for the past year but did not know YAZ's first or last name.

12. Members of the search team located the Subject Vehicle in a parking lot on the corner of Washington Street and Burnett Street, which is a short distance from RIOS-FRANCO's residence. Behind the driver's seat, in plain view, investigators saw a yellow bottle of HEET. HEET is a fuel additive that is commonly used to wash hand-written ink from checks. I also saw on the front passenger seat, a black jacket resembling the Moncler-brand jacket worn by RIOS-FRANCO days prior to the execution of the search warrant. The Subject Vehicle was towed to Boston Police District B-2 and impounded pending the application of these search warrants.

The Use of Rental Cars Associated with A&E Lux Auto, LLC to Commit Mail Theft

13. I am aware of multiple instances of mail theft that have occurred since October 2023, involving vehicles registered to Andrei Echeverria of A&E Lux Auto, LLC. For example, on October 30, 2023, a blue Audi bearing Massachusetts Registration 1EML67 was used in a mail theft incident in Wellesley. An image of this vehicle and a subject stealing mail is below.



14. On November 27, 2023, Wellesley PD and Newton PD pursued a red BMW bearing Massachusetts Registration 2RDJ15 after a mail theft incident outside of the Grove Street Post Office in Wellesley. The pursuit ended when the red BMW crashed. Two individuals were arrested and hundreds of pieces of mail from several communities, including Newton and Wellesley, were recovered from the red BMW.² An image of this vehicle and a subject stealing mail is below.

² This incident is under investigation and at this time there is no known affiliation between RIOS-FRANCO or co-conspirators with the individuals arrested on November 27, 2023.



15. Both the blue Audi and red BMW are registered to Andrei Echeverria of A&E Lux Auto, LLC, the same owner as the Subject Vehicle.

16. Based on my training and experience, the evidence seized from RIOS-FRANCO's residence (including the key fob to the Subject Vehicle), and the HEET observed in the Subject Vehicle, I believe that RIOS-FRANCO and others used the Subject Vehicle to commit the Target Offenses. I further believe that information from the equipment inside the Subject Vehicle will contain evidence of the Target Offenses, described in Attachment B-2. A description of the equipment and the information capable of being stored on such systems is below.

**BACKGROUND REGARDING THE SUBJECT VEHICLE AND ITS INFOTAINMENT
AND TELEMATICS SYSTEMS**

17. Based on my training and experience, and discussions with other experienced law enforcement officers and witnesses, the Subject Vehicle's infotainment and telematic systems (the "equipment") collects data regarding the Subject Vehicle's use and other electronic devices connected to it.

18. Berla.co is a leading provider of vehicle information forensic software. Berla's website and application allows investigators to search by make, model and VIN number and will provide a report of the information that can be forensically recovered from a vehicle. These systems are designed to store data which includes recent destinations, favorite locations, call logs, contact lists, SMS messages, emails, pictures, videos, social media feeds, and the navigation history of the vehicle. These systems may also record events such as the activation and de-activation of the vehicle's headlights, the opening and closing of doors at a specific location, and the location of the vehicle at the time Bluetooth devices are connected. The Subject Vehicle's equipment is capable of storing the following information:

- a. Electronic devices connected to the Subject Vehicle;
- b. Phones connected to the Subject Vehicle;
- c. Unique identifiers of the phones connected to the Subject Vehicle;
- d. Contacts;
- e. Call logs;
- f. SMS messages;
- g. Media files;
- h. CD/DVD history;
- i. Traffic updates;
- j. Navigation history;
- k. Favorite and/or recent locations;
- l. Bluetooth connections; and
- m. USB connections.

19. Based on my training and experience, and discussions with other experienced law enforcement officers and witnesses, I have also learned that:

- a. Many modern motor vehicles are equipped with sensors, cameras,³ transmitters, and electronic control units (“ECUs”)⁴ to monitor and manage vehicle operations, track vehicle movement, and exchange information with other vehicles and infrastructure.⁵ These systems also enable motor vehicles to interface with various types of mobile devices to facilitate the use of applications, including third-party navigation, hands-free phone calls, multimedia streaming, and other features.
- b. Two commonly installed ECUs within motor vehicles are infotainment and telematics systems—sometimes referred to as the Telematics Control Unit and the Infotainment Control Unit. These systems typically retain user data within the vehicle.
- c. A vehicle’s infotainment system combines hardware and software to provide entertainment features. Many infotainment systems allow drivers

3 As of 2018, the US National Highway Safety Transportation Agency requires new motor vehicles sold in the United States to have backup cameras installed by the manufacturer.

4 “ECU” is a generic term applied to any embedded computer that controls one or more electrical systems within a vehicle. ECUs are typically installed in a vehicle by the original equipment manufacturer during the manufacturing process. There are many types of ECUs, and as vehicles have more features each year, the number of ECUs in each motor vehicle increases. Newer motor vehicles can integrate as many as 150 ECUs, ensuring, in theory, that each part of the motor vehicle is running properly. Some examples of common ECUs include the Engine Control Module, Transmission Control Module, Brake Control Module, and Suspension Control Module, as well as the Telematics Control Unit and Infotainment Control Unit.

5 The infotainment and telematics systems in motor vehicles are not the same as “black box” recorders. Black box recorders are called event data recorders (EDRs) or crash data recorders. These black box recorders can record vehicle speed, engine speed, steering angle, throttle position, braking status, force of impact, seatbelt status, and airbag deployment. In 2006, the US National Highway Traffic Safety Administration (NHTSA) adopted regulations requiring EDRs to uniformly collect certain crash data to assist crash investigators with accident reconstruction efforts. In 2012, NHTSA proposed requiring manufacturers to install EDRs in all new cars and trucks, but in 2019, the NHTSA withdrew the proposal because automakers have voluntarily installed the devices in nearly all vehicles.

and passengers to connect their mobile electronic devices to the vehicle. When connected, the driver and/or passengers may gain access to, for example, Global Positioning System (GPS) navigation, video players, music streaming, voice calling, texting, and traffic data. Many systems enable talking hands-free with Bluetooth connectivity, listening to music, watching videos, or navigation. Many of these features are accessible via the (usually interactive) console located on the front dashboard of the vehicle.

- d. A vehicle's telematics system typically collects and stores diagnostic data from various systems (other ECUs) within the vehicle, including historical navigation points, speed, and event data. Historical event data may include information regarding when the car's trunk, doors, and windows opened and closed, when headlights turned on and off, and when gears changed, or brakes were engaged.
- e. The main difference between the infotainment and telematics systems is that the infotainment system is about entertainment for the occupants of the vehicle, and the telematics system is for collecting and reporting (transmitting) information—such as vehicle use data, maintenance requirements, and automotive servicing—about the vehicle. Typical telematics data may include turn-by-turn navigation, remote access, emergency calling, and maintenance notifications. Examples of vehicle telematics systems include General Motors' OnStar, BMW's "Assist," and Mercedes' "mbrace." Some of these systems are integrated multimedia

navigation and telematics systems in one (combined infotainment/telematics systems), like Toyota's "Entune" and Ford's "Sync."

- f. The data generated, collected, transmitted, and retained by motor vehicles can provide valuable information in law enforcement investigations of crimes. For example, many infotainment systems support the importation of content and other data information from a particular user's mobile device. Such data may include content that may provide attribution to particular user(s), including mobile device identifiers, wireless telephone numbers, user account details, passwords, user voice profiles, contact lists, call logs, text messages, pictures, e-mail, videos, web history, GPS coordinates, and other historical navigation information.
- g. I am aware that the ECUs within many motor vehicles store data for prolonged periods of time. Furthermore, even after a previously connected mobile device is removed from the physical vehicle, data may remain within the ECU. Such stored data can be used to identify locations, victims, witnesses, associates, and co-conspirators and may include communications and images of criminal activity. In sum, a forensic examination of a motor vehicle's infotainment and telematics systems may reveal the vehicle's GPS location information, movements, operations, and user data at critical moments before, during, and after the commission of a crime.
- h. The Subject Vehicle has an infotainment and telematic system (the "equipment"). To complete a forensic extraction of the equipment, it may

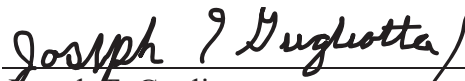
be necessary, temporarily, to remove trim and other components of the Subject Vehicle to access the equipment. It may also be necessary to repair the equipment, replace the screen, reconnect wires, and replace batteries. It may be necessary to employ advanced forensic processes to bypass locked display screens and other data access restrictions. Advanced processes may include potentially destructive forensic techniques used to remove memory chips from computers and other electronic storage containers that may be found within the equipment and Subject Vehicle. In the event that potentially destructive processes are required to perform this extraction, parts of the Subject Vehicle may be destroyed and rendered useless.

- i. Furthermore, it may be necessary to return to the Subject Vehicle and reconnect the equipment to the Subject Vehicle's power source to perform the extraction using forensic software. This is because there are various computer networks working simultaneously when a vehicle is powered on, and in some vehicles, the infotainment and telematics systems require the other networks to work in tandem to complete the data extraction.
- j. The requested warrant authorizes a later review of the data seized or copied from the equipment, which review may continue past the date required for execution of the warrant.

CONCLUSION

20. I have probable cause to believe that evidence, fruits, and instrumentalities of the Target Offenses, as described in Attachments B-1 and B-2, are contained in the Subject Vehicle described in Attachment A-1 and the equipment described in Attachment B-2.


Respectfully submitted,



Joseph T. Gugliotta
Postal Inspector
United States Postal Inspection Service

Signed electronically and sworn to via telephone in accordance with Federal Rule of Criminal Procedure 4.1 on this 15th day of March 2024.

2:20 p.m.



The Honorable David R. Kennedy
United States Magistrate Judge
District of Massachusetts



Attachment A-1

Property to be Searched

A 2018 BMW X6 with VIN 5UXKU2C53J0Z61448 and Massachusetts Registration 1WYZ17 (“the Subject Vehicle”) that currently is stored securely at Boston Police District B-2, 2400 Washington Street, Roxbury, Massachusetts 02119.

Attachment A-2

Property to be Searched

Infotainment System from the Subject Vehicle

The infotainment and telematic systems (the “equipment”) of a 2018 BMW X6 with VIN 5UXKU2C53J0Z61448 and Massachusetts Registration 1WYZ17 (“the Subject Vehicle”) that currently is stored securely at Boston Police District B-2, 2400 Washington Street, Roxbury, Massachusetts 02119.

Attachment B-1

Items to be Seized

Any and all property that establishes custody or occupancy of the Subject Vehicle or involves violations of 18 U.S.C. §1704 (Theft or Forging of Postal Service Keys), 18 U.S.C. § 1708 (Theft or Receipt of Stolen Mail), 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1344 (Bank Fraud), and 18 U.S.C § 371 (Conspiracy) from January 2023 to present, including:

1. Rental records;
2. Implements or devices used to steal or “fish” mail from collection boxes;
3. Financial instruments, including checks and money orders;
4. ATM deposit slip and withdrawal receipts, as well as other financial records or notes involving financial transactions;
5. Notes or records pertaining to communication between Imanol RIOS-FRANCO and other individuals that relate to the above-mentioned offenses;
6. HEET or other substances used to wash hand-written ink and any containers that could be used for washing ink.
7. Debit, credit, or gift cards in names other than RIOS-FRANCO;
8. Notes, records, or communications pertaining to mobile banking access including usernames, passwords, and challenge questions;
9. Stolen U.S. mail, including mail not addressed to RIOS-FRANCO;
10. Stolen checks, including checks payable to or drawn from accounts ^{Related} ~~unrelated~~ to individuals other than RIOS-FRANCO;
11. USPS Arrow Keys or counterfeit Arrow Keys; *David H. Kennedy*
12. US currency related to income derived from bank fraud or wire fraud;
13. Records and tangible objects pertaining to the payment, receipt, transfer, or storage of money or other things of value by RIOS-FRANCO, including:

- a. Bank, credit union, investment, money transfer, and other financial account information;
 - b. Credit and debit card account information;
 - c. Tax statements and returns;
 - d. Business or personal expenses;
 - e. Income, whether from wages or investments; and
 - f. Loan applications and related documents.
14. Records and tangible objects pertaining to the travel of RIOS-FRANCO between July 1, 2023 and October 20, 2023;
15. Clothing items and accessories as depicted in the CCTV footage throughout the investigation, including:
 - a. A gray sweatshirt with the green writing “Spy5er” depicted below:



- b. A cellphone case with “Sprinklez” and black/white stickers as depicted below:



Attachment B-2

Items to be Seized

Any information regarding violations of 18 U.S.C. §1704 (Theft or Forging of Postal Service Keys), 18 U.S.C. § 1708 (Theft or Receipt of Stolen Mail), 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1344 (Bank Fraud), and 18 U.S.C § 371 (Conspiracy) from January 2023 to present, including:

1. Records pertaining to communications between Imanol RIOS-FRANCO and other individuals, related to the above-mentioned offenses;
2. Records that identify device(s) connected to the equipment, and records identifying the user(s) of those device(s);
3. Data, information, images, and vehicle diagnostic data from the equipment, related to the above-mentioned offenses, including:
 - a. Electronic devices connected to the Subject Vehicle;
 - b. Phones connected to the Subject Vehicle;
 - c. Unique identifiers of the phones connected to the Subject Vehicle;
 - d. Contacts;
 - e. Call logs;
 - f. SMS messages;
 - g. Media files;
 - h. Traffic updates;
 - i. Navigation history;
 - j. Favorite and/or recent locations;
 - k. Bluetooth connections; and
 - l. USB connections.